(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2001 (28.06.2001)

PCT

(10) International Publication Number
WO 01/46773 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US00/34423

(22) International Filing Date:
19 December 2000 (19.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/172,857 20 December 1999 (20.12.1999) US
09/693,540 20 October 2000 (20.10.2000) US

(71) Applicant: EVELOCITY CORPORATION [US/US]; One Pine Crest Terrace, Pease International Tradeport, Portsmouth, NH 03801 (US).

(72) Inventors: SCHWARTZ, Richard; 12 Lacy Lane, Nashua, NH 03062 (US). PERRY, Bruce; 328 South Street, Chestnut Hill, MA 02467 (US).

(74) Agents: POWSNER, David, J. et al.; Nutter, McClennen & Fish LLP, One International Place, Boston, MA 02110-2699 (US).

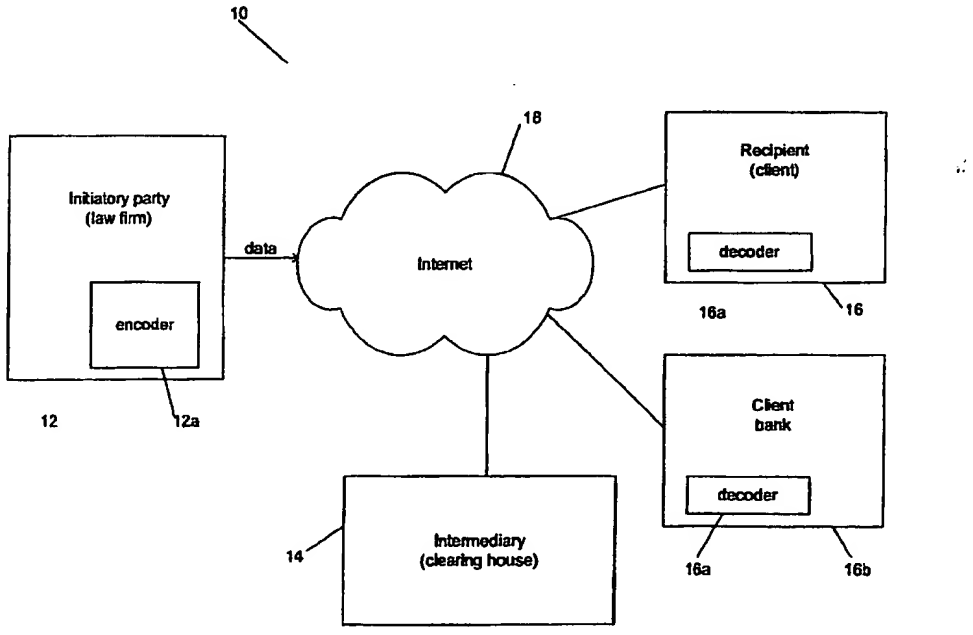
(81) Designated States *(national)*: AU, CA, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR TRANSMITTING DATA



(57) Abstract: The present invention provides methods and system for encrypting and transmitting data to a recipient. More particularly, the method of the invention allows encrypting selected portions of data stream that is sent to a recipient authorized to decrypt the encrypted portions via a third party intermediary who is not authorized to decrypt the encrypted portions.

WO 01/46773 A2

METHOD AND APPARATUS FOR TRANSMITTING DATA

Related Applications

This applications claims priority to U.S. Serial Number 09/693,540, filed October 20, 2000, entitled "Method and Apparatus for Transmitting Data," and U.S. Serial Number 60/172,857, filed December 20, 1999, entitled "Method and apparatus for transmitting data," the teachings of both of which are incorporated herein by reference.

Background of the Invention

The present invention relates generally to digital data processing, and more particularly, to methods and systems for transmitting data to a recipient. More particularly, the invention provides methods and systems for ensuring the security of privileged information when data is transmitted to a recipient via a third party intermediary.

The exchange of data through public networks and/or third party intermediary services raises issues of security. Such is the case, for example, in communications between lawyers and their clients, e.g., over the Internet. A breach in the security of those communications may lead to disclosure of the client's secrets, as well as the loss of certain legal testimonial privileges. The use of "secure channels", e.g., SSL, Lotus Domino port encryption, may not always be sufficient to overcome these concerns. For example, when a third party intermediary participates in data exchange between two parties, its computers may store data received from the sender (e.g., for processing or conversion), prior to forwarding it to the recipient.

The intermediary may employ a variety of techniques, such as database access controls, firewalls, virtual private networks, encrypted disk storage, to protect the stored data. Such measures, however, are typically not sufficient to ensure that the data remains secure. For example, such measures may not protect sensitive data from disclosure to intermediary's employees, or to the operators of the outsourced systems, when the intermediary processes the data.

Encrypting the entirety of the data submitted to an intermediary may defeat its very role. It may, for example, prevent the intermediary from processing selected portions of the data.

An object of the invention is to provide improved methods and systems of digital data processing. A more particular object is to provide such methods to facilitate transmission of data, e.g., through public networks and/or third party intermediaries.

A related object of the present invention is to provide methods and systems for encrypting a stream of data such that an intermediary can perform the requisite processing of the data while ensuring that the privileged information remains secure.

A further object of the invention is to provide such methods and systems as to improve the security of data maintained within a site, e.g., even if not transmitted across a network or through an intermediary.

Still other objects of the invention are to provide such methods as can be readily utilized with existing data processing systems and technologies.

Still another object of the invention is to provide such methods as can be implemented at low cost and with little processing or other overhead.

Summary of the Invention

The present invention provides a method for transmitting a stream of data, such as textual data, to a recipient. In a first step, at least one selected segment of the data is encrypted before its transmission to the recipient. The term segment as used herein can refer to one or more fields within a record of the data. Alternatively, the term segment can refer to one or more records of the data. In a second step, the encrypted segment is identified by an identification tag that provides encryption attributes of the encrypted segment.

When the encrypted segment is at least one field within a selected record, the identification tag can be employed to demark a record within which the encrypted field resides. Alternatively, the identification tag can be employed to demark the encrypted field directly. In either case, the identification tag identifies the encrypted segment and further provides various encryption attributes thereof, as discussed below. Moreover, the identification tag can include one or more identifiers that bind the encrypted segment to meta-data provided, for example, elsewhere in the stream of data sent to a recipient. The meta-data provides the attributes of the encrypted segment.

In one aspect of the invention, the stream of data contains invoice information, such as an invoice of a law firm, that is sent to a recipient, for example, a client of the law firm, via an intermediary, such a clearinghouse. The clearinghouse can receive the invoice electronically, and can process selected information within the invoice before transmitting it to the client. The method of invention allows encrypting selected portions of the data to prevent the intermediary, e.g., clearinghouse, from having access to these portions. That is, the intermediary can process a portion of the data without having access to those portions of the data that contain sensitive and/or privileged information, and hence must be protected from parties other than the end-user, e.g., the client of the law firm. After receiving the data, the intermediary transmits the data, with or without any additional processing, to the intended recipient.

In a related aspect, a public key of a recipient or a shared secret key known to the intended recipient is employed to encrypt selected segments of the data. A number of known algorithms can be employed to encrypt these selected segments. These algorithms include, but are not limited to, DES, RC2, RC4, RC5, Triple-DES, Blowfish, Diffe-Hellman, and PGP.

According to another aspect, a public key is used to encrypt a secret session key, which is then employed to encrypt selected segments of the data. Alternatively, a portion of the session key, for example, a pre-defined number of sequential bits of the session key can be employed to encrypt the selected segments. The selected sequential bits of the key can begin, for example, with the first bit of the session key.

An intended recipient of the data authorized to access the encrypted data, such as a client of a law firm, needs information regarding which segments are encrypted, and the method employed for encrypting these segments, to be able to decrypt them. The invention provides identification tags to convey this information to the recipient. An identification tag not only identifies at least an encrypted segment, but it also provides the encryption attributes of the encrypted segment to allow the intended recipient to decrypt it. The encryption attributes can include a type attribute that indicates whether a public key or a secret key is employed for encrypting the segment, and a decrypting party attribute that indicates the party whose key was employed for encrypting the segment. The party whose key was employed is typically the intended recipient. Further, a cipher attribute indicates the encryption algorithm employed for encrypting the segment.

In a related aspect, a segment is encrypted in a binary format. The encrypted segment can then be encoded from the binary format into an ASCII format by employing a known algorithm. In such a case, an identification tag that identifies the encrypted segment includes, in addition to the information discussed above, a representation attribute which identifies the algorithm employed for encoding the binary format into an ASCII format.

In another aspect, the present invention employs a mark-up language, such as HTML, XHTML or XML, to format a plurality of records such that a pair of tags of the mark-up language demark one or more records of data having at least an encrypted segment, for example, one encrypted field. That is, the tags of the mark-up language are employed to provide identification tags for identifying encrypted segments and for providing their encryption attributes.

A system for implementing the method of the invention can include an encoder for encoding selected segments of data to be transmitted to an intended recipient. The encoder can employ either a public key of a recipient or a secret key also known to the recipient, and supplied to the entity transmitting the data to an intermediary, to encode the selected segments. Each segment can be, for example, a field within a record of the data. The encoder can employ a mark-up language, such as HTML or XML, to demark each record within which at least one encrypted field resides with an identification tag. The identification tag identifies each encrypted field within the record and further provides its encryption attributes, as discussed above.

The data having the encrypted segments can be sent to an intermediary, such as a clearinghouse, through a communication channel that provides connection to a network, such as the Internet, to which the intermediary is connected. Upon the receipt of the data, the intermediary can, if warranted, process selected portions of the non-encrypted segments of the received data, and transmit the entire data, i.e., both the encrypted and the non-encrypted segments, to the intended recipient. In one aspect, the intermediary and the intended recipient can communicate with each other and exchange data through the Internet. Those skilled in the art will appreciate that other modes of communication can be employed to transfer data between the various parties.

The recipient can employ the identification tags to identify and to decrypt the encrypted segments of the data. Thus, the invention allows the intermediary to provide any necessary processing of non-privileged portions of the data without compromising the security of the privileged portions of the data.

Illustrative embodiments of the invention will be described below relative to the following drawings.

Brief Description of the Drawings

FIGURE 1 schematically illustrates a system for implementing a data transmission method accordingly to the teachings of the invention, and

FIGURE 2 schematically illustrates a system for providing flow of data, encrypted according to the teachings of the invention, among a law firm, a third party intermediary and a client of the firm and/or the client's bank.

Detailed Description of the Illustrated Embodiment

The present invention provides methods and system for encrypting selected segments of a stream of data, and transmitting the data having the encrypted segments to a recipient. In preferred embodiments of the invention described below, the data having the encrypted segments is first transmitted to an intermediary who subsequently transmits the data to an intended recipient who is authorized to de-crypt the encrypted portions. The intermediary can not de-crypt the encrypted segments but can process the non-encrypted portions of the data, if warranted, before transmitting the data to the intended recipient. The intended recipient, however, can de-crypt the encrypted segments to have access to the entire data.

FIGURE 1 illustrates an exemplary system 10 for implementing the method of the invention. An initiating party 12, such as a law firm, can transfer data to an intermediary 14, such as a clearinghouse, and/or to an intended recipient 16, such a client bank, through a messaging network 18, e.g., the Internet. Further, the intermediary 14 and the recipient 16 can exchange data through the Internet.

Without any loss of generality and only for the purposes of illustration, the initiating party in this illustrative example is a law firm that transmits invoice data to the clearinghouse 14. The initiating party 12 can employ, for example, an encoder 12a to encrypt selected segments of the invoice data according to the teachings of the invention to secure sensitive and/or privileged information from the clearinghouse. The clearinghouse may process the non-encrypted portions of the invoice data, and subsequently transmit the data to the client or a client bank 16b. The client 16 or the client bank 16b can employ a decoder 16a to de-crypt the encrypted portions of the data.

The law firm may utilize a computerized billing system to generate invoices based on attorney timesheets and disbursement recordals. The invoices are electronically transmitted to the clearinghouse 14, for example, to a computer 20 at the clearinghouse 14 (FIGURE 2). The central clearinghouse computer 20, for example, maps the invoice data to a standard format and compares

invoiced amounts with pre-approved amounts for automatic approval. Where the invoiced amounts compare favorably with pre-approved amounts, the computer 20 generates accounts receivable (A/R) and accounts payable (A/P) transactions for communication to the law firm and to client computer 22, respectively. In addition, the central clearinghouse computer 20 stores the transaction in a database for tracking and reporting.

Computer 22 of the client 16 receives the A/P transaction report and issues electronic payment instructions to the clients bank. Alternatively, payment instructions may be issued to bank 16b directly by central clearinghouse computer 20. On receipt of the payment instruction, the client's bank initiates a funds transfer to the law firm.

If the invoiced amounts do not compare favorably with the pre-approved amounts, the computer 20 generates a report for transmittal to the law firm computer 12a and to client computer 22. On receipt of such report, representative of the service provider 14 and client 16 can communicate, e.g., via phone, e-mail, etc, to resolve any potential dispute.

The method of the invention allows the law firm to encrypt selected segments of the invoice data containing privileged and/or sensitive information before transmitting it to the clearinghouse. This prevents the clearinghouse from having access to such privileged information while being able to process the non-encrypted portions of the data.

In a preferred embodiment of the invention, a mark-up language, such as XML or HTML or a variant of HTML (e.g., XHTML), is employed to format the data so as to identify the segments that have been encrypted. An encrypted segment, for example, can correspond to a field within a record, or an entire record. For example, a pair of tags of the mark-up language can de-limit each record having at least an encrypted field. The tags can identify the encrypted field and further provide encryption attributes thereof. For example, a <CRYPTO>... </CRYPTO> tag pair can indicate that at least a segment of data enclosed between the tag pair is encrypted. That is, if no <CRYPTO>... </CRYPTO> tag pair occurs within a data stream, no encryption is done.

Both public key and secret key cryptography can be employed for encrypting selected segments of the data stream. In secret key cryptography, an initiating party and an intended recipient who is authorized to de-crypt the data agree on one or more secret keys. In public key cryptography, the initiating party utilizes a published key of an intended recipient to encrypt selected segments of the data, and the intended recipient employs a corresponding private key, known only to the intended recipient, to de-crypt the data.

When secret key cryptography is employed, the method of the invention provides the following exemplary syntax to de-limit a section of the data stream, e.g., a record, with a<CRYPTO>... </CRYPTO>tag pair and to identify one or more secret cryptography keys and to bind each of them to a particular cipher:

<CRYPTO type = 'secret' cipher = 'string-ciphername' representation = 'string-repname [keylength = 'number']>

<CRYPTO_SECRET_KEY id = 'string' name='string'>

<CRYPTO_SECRET_KEY id = 'string' name='string'>

...

</CRYPTO>

The above tag pair provides the various attributes of an encypted segment identified by the tag pair. In particular, a type attribute can indicate whether secret or public cryptography is employed. In this illustrative example, the type attribute indicates that secret cryptography is utilized. The cipher attribute takes a string argument, i.e., string-ciphername, which indicates the particular cryptographic algorithm that is utilized. For example, the string-ciphername can indicate that a DES, or an RC2, or an RC5 algorithm is employed to encrypt a segment identified by the tag pair.

The output from a cryptographic algorithm is typically in the form of binary data. It may be desirable to encode this binary data into an ASCII format. A number of methods, such as base64 or binhex, are known for effectuating such a transformation of binary data into ASCII format. The

above illustrative syntax provides a representation attribute that indicates the type of method employed for transforming the coded binary data into ASCII format. In particular, the representation attribute has a string argument, herein referred to as string-repname, that identifies the transformation method.

In certain cases, the initiating party and the intended recipient can agree on a very long key, but employ a subset of the key for encrypting selected segments of the data. This can provide significant advantages in that different subsets of the same long key can be employed, if needed, without exchanging a new key between the parties. For example, if government regulations regarding the security level of cryptographic data are changed, a different subset, for example a larger subset, can be employed without a need for exchanging a new key between the initiating party and the recipient. The above illustrative syntax includes a keylength attribute that identifies the number of bits in the secret key that were employed for encryption.

The above illustrative syntax further includes a <CRYPTO_SECRET_KEY> tag that provides a name attribute for informing a recipient, who is authorized to decipher the encoded data, which secret key was employed. It is clear that the key itself is not disclosed, but rather the name attribute provides a reference to the key. The parties agree in advance of exchange of information on such a reference.

Moreover, the above syntax includes an identification ('id") attribute that relates the meta data provided between within the <CRYPTO_SECRET_KEY> tag to encrypted data that occurs in the stream of the transmitted data.

The above syntax illustrates that multiple <CRYPTO_SECRET_KEY> tags can be provided within a data stream to allow an exchange of data between three or more parties in such a way that each party has access to only a subset of the data.

Further, multiple <CRYPTO> ... </CRYPTO> tag pairs can be provided within the same data stream to allow the use of multiple encryption types and/or ciphers within the data stream.

In public key cryptography, a party who wishes to receive encoded information can publish a key in a publicly accessible directory. The public key can be utilized to encode data destined for the party. The encoded information can be decoded only by employing a private key corresponding to the public key, which is known only to the party who published the public key.

The present invention can be employed to encode selected segments of a data stream by employing public key cryptography. In addition, a hybrid technique can be utilized in which a public key is used only to encrypt a session key, which has less number of bits than the public key. The session key is then employed to encode selected segments of the data stream. Because encoding algorithms for secret key cryptography are typically many times faster than those for public key cryptography, the use of such a hybrid technique allows the parties to encode and/or decode selected segments of the data more efficiently.

An exemplary syntax provided by the present invention for public key cryptography is as follows:

<CRYPTO type = 'public' keycipher = 'string-ciphername' keyrep = 'string-repname' cipher = 'string-ciphername' representation = 'string-repname'
[keylength = 'number'] [sessionkeylength = 'number']>
<CRYPTO_SESSION_KEY id = 'string' directory = 'string'>
<CRYPTO_KEY_EXCHANGE recipient= 'string'>'string'
</CRYPTO_KEY_EXCHANGE>
...
</CRYPTO_SESSION_KEY>
</CRYPTO>

In the above illustrative syntax, the type attribute can be either public or secret, indicating the type of cryptographic method utilized to encode the data segments identified by the <CRYPTO>... </CRYPTO> tag pair. In this example, public key cryptography is chosen for encoding a session key, which in turn is employed to encode selected segments of a data stream.

A keycipher attribute takes a string argument, i.e., string-ciphername, that identifies the public key cryptographic algorithm, e.g., RSA, that is employed for encoding a session key. The output of such an algorithm is typically in the from of a binary data stream that can not be included in an XML data stream. Hence, it is typically necessary to convert the coded binary data into an ASCII stream. A keyrep attribute having a string argument,e.g., string-repname, identifies methods for encoding binary data into an ASCII stream. Such methods can include, for example, base64, binhex, etc.

The parties who exchange information through encoded data can agree to employ selected bits of a large public key to encode a secret session key. Further, the parties can agree on employing a selected portion, i.e., selected number of bits, of a session key to encode selected segments of a data stream.

The above syntax can be employed to inform the party who receives the encoded data how many bits of the public and/or the secret session key were in fact employed for encryption. In particular, in the above illustrative syntax, the keylength attribute indicates the number of bits in a large public key that were employed to encode a secret session key. Further, the sessionkeylength attribute indicates the number of bits in a secret session key that were employed to encode selected segments of the data stream.

The use of a secret session key allows encrypting selected segments of a data stream by employing a secret key cryptographic algorithm. In this exemplary embodiment, a cipher attribute identifies the algorithm employed for encrypting the data. Such algorithms can include, but are not

limited to, DES, RC2, and RC5. Further, the representation attribute identifies the method employed to convert the encoded binary data into ASCII format.

In the above example, a <CRYPTO_SESSION_KEY>...</CRYPTO_SESSION_KEY> tag pair delimits a plurality of encrypted session keys. Further, a directory attribute specifies the name of a directory agreed upon by the parties as the source of public keys that can be employed for encrypting the session keys. The id attribute relates the meta-data to the encrypted data that occurs within the data stream.

A plurality of <CRYPTO_KEY_EXCHANGE>...</CRYPTO_KEY_EXCHANGE> tag pairs de-limit multiple instances of the same session key. Each instance of the session key is encoded by employing a public key of one of the recipients, which is identified in the tag pair. In particular, the recipient attribute identifies a recipient who is authorized to decrypt an instance of the session key.

In some cases, all or significant portions of a data stream need to be encoded. The method of the invention provides a default syntax that can be optionally employed in such situations to inform a recipient of encryption attributes of these portions of data. In particular, an optional <CRYPTO_DEFAULT id = 'string'> tag can be provided in the data stream to indicate that all subsequent data elements are encoded by employing a <CRYPTO_SECRET_KEY> or a <CRYPTO_SESSION_KEY> whose id attribute matches the string specified in the id attribute of the <CRYPTO_DEFAULT> key. A default tag can be overridden by employing a CRYPTO attribute, e.g., a <CRYPTO>...<\CRYPTO> tag pairs.

The method of the present invention is particularly suited for use in conjunction with a mark-up language, e.g., XML or HTML, for identifying encrypted portions of a data stream, and for identifying the encryption attributes of these portions. For example, when XML mark-up language is employed, every XML tag pair that directly encloses data can be configured to support an optional CRYPTO attribute, which specifies a string argument. A value of '0' for this string

argument can be reserved to indicate that the data enclosed within the XML tag pair is not encrypted. Any other value of this string argument is chosen to match the id attribute of a preceding <CRYPTO_SECRET_KEY> or <CRYPTO_SESSION_KEY> tag, which provide the key, the cipher, and the representation employed for encrypting the data within the XML tag pair, as discussed above.

It is also possible to employ an XML tag pair to enclose a block of tags, each of which encloses some portion of a data stream. Such an XML tag pair can also be configured to include an optional CRYPTO attribute, which specifies a string argument. If the value of the string argument is set to '0', the data enclosed within the tag pair is not encrypted. Any other value of the string argument indicates that the enclosed data is in fact encrypted. A non-zero value of the CRYPTO attribute can be selected to match the id attribute of, for example, a preceding <CRYPTO_SECRET_KEY> or <CRYPTO_SESSION_KEY> tag, thereby indicating the key, the cipher, and the representation employed for encrypting the data.

The following example further illustrates the method of the invention for encoding selected portions of a stream of data.

EXAMPLE

```
<CRYPTO type='public' keycipher = 'RSA' keyrep = 'base64' cipher = 'RC4' representation = 'base64' keylength
= '512' sessionkeylength = '40'>
<CRYPTO_SESSION_KEY id ='code-1' directory = 'eV-LADP1'>
    <CRYPTO_KEY_EXCHANGE recipient = 'firm-1'>123456789</CRYPTO_KEY_EXCHANGE>
    <CRYPTO_KEY_EXCHANGE recipient ='clnt-1'>987654231</CRYPTO_KEY_EXCHANGE>
</CRYPTO_SESSION_KEY>
</CRYPTO_SESSION_KEY id = 'code-2' directory = 'eV-LDAP1'>
    <CRYPTO_KEY_EXCHANGE recipient = 'firm-1'>asdfghjkl</CRYPTO_KEY_EXCHANGE>
    <CRYPTO_KEY_EXCHANGE recipient = 'clnt-1'>lkjhgfdsa</CRYPTO_KEY_EXCHANGE>
</CRYPTO_SESSION_KEY>
</CRYPTO>
```

```
...
<CRYPTO_DEFAULT id = 'code-1'>
...
<!-first fee->
<FEE>
...
        <FEE_TASK_DESC>1jj89kjds3f10ksdj90dsjfk34sdj90149a4ds6ja7sd</FEE_TASK_DESC>
</FEE>
...
<!-second fee->
<FEE>
...
   <FEE_TASK_DESC crypto='0'>Telephone conference with adjuster re schedule IME with Dr. Slaughter.
</FEE_TAKS_DESC>
</FEE>

<!-third fee->
<FEE>
...
   <FEE_TASK_DESC crypto = 'code-2'>2AklaDA3s3JDL64KA4JSdkslfkds</FEE_TASK_DESC>
</FEE>
...
<!-fourth fee->
<FEE crypto = '0'>
...
   <FEE_TASK_DESC>another telephone conference with adjuster re schedule IME with Dr.
Slaughter.</FEE_TASK_DESC>
</FEE>
<!-fifth fee->
<FEE crypto = 'code-2'>
...
   <FEE_TASK_DESC>2AklaDA3S3JDL64KA4JSdkslfkds</FEE_TASK_DESC>
</FEE>
<!-fifth fee->
<FEE crypto='code-2'>
...
```

```
    <FEE_TASK_DESC>2AklaDA3S3JDL64KA4JSdkslfkds</FEE_TASK_DESC>
</FEE>
<!-sixth fee->
<FEE CRYPTO = '0'>
...
    <FEE_TASK_DESC crypto = 'code-1'>ds1jf31askldas1kdaa78dfl14aks</FEE_TASK_DESC>
</FEE>
```

In the above example, the first <FEE_TASK_DESC>...</FEE_TASK_DESC> tag pair does not include a CRYPTO attribute. Hence, the data enclosed within this tag pair is encrypted in accord with the default tag provided above this tag pair. The id attribute of the default tag in conjunction with the information provided within the <CRYPTO>...</CRYPTO> tag pair indicate that the data contained within the first <FEE_TASK_DESC>...</FEE_TASK_DESC> tag pair is encrypted by employing an RSA/RC4 hybrid cryptosystem. That is, a session key identified as 'code-1' is encrypted by employing the RSA public cryptography algorithm. Subsequently, this session key and the RC2 cryptography algorithm are utilized to encode the data.

The second <FEE_TASK_DESC>...</FEE_TASK_DESC>tag pair includes a CRYPTO attribute that is set to '0', indicating that the data contained within this tag pair is not encrypted.

The CRYPTO attribute of the this <FEE_TASK_DESC>...</FEE_TASK_DESC> tag pair is set to 'code-2'. This indicates that the data enclosed within this tag pair is encrypted by employing a session key identified as 'code-2', and an RSA/RC4 hybrid cryptosystem.

The fourth <FEE_TASK_DESC>...</FEE_TASK_DESC>tag pair has no CRYPTO attribute. However, this tag pair is enclosed within a <FEE>...</FEE> tag pair that includes a CRYPTO attribute that is set to '0'. Hence, the data within the fourth <FEE_TASK_DESC>...</FEE_TASK_DESC> is not encrypted.

The fifth <FEE_TASK_DESC>...</FEE_TASK_DESC>tag pair includes no CRYPTO attribute. However, this tag pair is enclosed within a <FEE>...</FEE> tag pair that has a CRYPTO attribute that is set to 'code-2'. Hence, the data within the fifth <FEE_TASK_DESC>...</FEE_TASK_DESC> is encrypted by employing a session key identified as 'code-2', and an RSA/RC4 hybrid cryptosystem.

The sixth <FEE_TASK_DESC>...</FEE_TASK_DESC> tag pair is enclosed within a <FEE>...</FEE>tag pair that includes a CRYPTO attribute having a value of '0'. The <FEE_TASK_DESC>...</FEE_TASK_DESC> tag pair, however, includes a CRYPTO attribute having a value of 'code-1'. The CRYPTO attribute of the <FEE_TASK_DESC>...</FEE_TASK_DESC> overrides that CRYPTO attribute of the <FEE>...</FEE> tag pair, and specifies that the enclosed data is encrypted by utilizing an RSA/RC4 hybrid cryptosystem and a session key identified as 'code-1'.

One skilled in the art will appreciate that various modifications to the above exemplary embodiments can be made without departing from the scope of the present invention, of which we claim:

1. A method for transmitting a stream of textual data to a recipient, the method comprising the steps of:

encrypting at least one selected segment of the stream of data,

identifying said encrypted segment by an identification tag, said tag providing encryption attributes of the encrypted segment.

2. The method of claim 1, wherein said selected segment includes at least one selected field in at least one selected record of the data.

3. The method of claim 2, wherein said step of identifying includes demarking said selected record with said identification tag.

4. The method of claim 2, wherein said step of identifying includes demarking said selected field with said identification tag.

5. The method of claim 1, wherein said stream of textual data includes information contained in a database.

6. The method of claim 5, wherein said database includes invoice information.

7. The method of claim 6, wherein said invoice information relates to a billing invoice of a law firm.

8. The method of claim 1, wherein the step of encrypting includes employing a public key and a selected encryption algorithm for encrypting said selected segment.

9. The method of claim 8, wherein said encryption algorithm is selected from the group consisting of DES, RC2, RC4, RC5, Triple-DES, Blowfish, Diffe-Hellman, and PGP algorithms.

10. The method of claim 1, wherein the step of encrypting includes employing a secret key and a selected encryption algorithm for encrypting said selected segment.

11. The method of claims 8, wherein the step of encrypting includes selecting a pre-defined set of bits in said public key to encrypt said selected segment.

12. The method of claim 10, wherein the step of encrypting includes selecting a pre-defined set of bits in said secret key to encrypt said selected segment.

13. The method of claim 1, wherein the attributes provided by said tag includes a type attribute indicating whether a public key or a secret key is employed for encrypting said selected segment.

14. The method of claim 1, wherein the attributes provided by said tag includes a cipher attribute indicating an encryption algorithm employed for encrypting said selected segment.

15. The method of claim 8, wherein the attributes provided by said tag includes a decrypting party attribute identifying the party whose public key was employed for encrypting said selected segment.

16. The method of claim 10, wherein the attributes provided by said tag includes an attribute for identifying a secret key known to the recipient.

17. The method of claim 1, wherein said step of encrypting includes the step of encrypting said selected segment in a binary format.

18. The method of claim 17, further comprising the step of encoding said encrypted binary segment into an ASCII format.

19. The method of claim 18, wherein the attributes provided by said tag includes a representation attribute identifying an algorithm employed for encoding the binary format into an ASCII format.

20. The method of claim 1, wherein said encrypting step includes employing a public key to encrypt a secret session key and employing the secret session key to encrypt said selected segment.

21. The method of claim 20, wherein the attributes provided by said tag includes a public key attribute identifying said public key and a session key attribute identifying said secret session key.

22. A method for transmitting a plurality of records to a recipient via an intermediary, each of said records including at least one field, the method comprising the steps of:

encrypting at least one field of at least one selected record, and

identifying said encrypted field by an identification tag, said tag providing encryption attributes of said encrypted field.

23. The method of claim 22, wherein said step of identifying includes demarking said selected record with said identification tag.

24. The method of claim 22, wherein said step of encrypting secures said encrypted field from the intermediary.

25. The method of claim 22, wherein said intermediary processes zero,one or more of said plurality of records other than said encrypted field and wherein said intermediary transmits said plurality of records to the recipient.

26. The method of claim 22, wherein said recipient can decrypt said encrypted field.

27. A method for transmitting a plurality of records to a recipient via an intermediary, each of said records containing at least one field, the method comprising the steps of:

encrypting at least one field of at least one of said records to secure the field from the intermediary,

employing a mark-up language to format said plurality of records such that a pair of tags of the mark-up language demarks the record having said encrypted field, said pair of tags providing encryption attributes of said encrypted field.

28. The method of claim 27, further comprising the step of selecting the mark-up language to be HTML.

29. The method of claim 27, further comprising the step of selecting the mark-up language to be XML.

30. The method of claim 27, further comprising the step of selecting the mark-up language to be XHTML.

31. A system for transmitting a stream of textual data to a recipient, comprising

an encoder for encrypting at least one selected segment of the stream of data and for identifying said selected segment by an identification tag, said tag providing encryption attributes of the segment it identifies,

and a communication channel for transmitting the data having said encrypted segment to the recipient.

32. The system of claim 31, wherein said encoder employs a public key and a selected encryption algorithm for encrypting said selected segment.

33. The system of claim 31, wherein said encoder employs a secret key and a selected encryption algorithm for encrypting said selected segment.

34. The system of claim 31, wherein said encoder employs a public key and a selected encryption algorithm to encrypt a secret session key and employs said secret session key and a selected encryption algorithm to encrypt said selected segment.

35. A system for transmitting a stream of data to a recipient via an intermediary, comprising

an encoder for encrypting at least one selected segment of the data to secure the encrypted segment from an intermediary and for identifying said encrypted segment by an identification tag which provides encryption attributes of said encrypted segment,

a first communication channel for transmitting the stream of data having said encrypted segment to the intermediary,

a processor operated by the intermediary for processing selected segments of non-encrypted portion of the data received by the intermediary to produce processed data,

a second communication channel for transmitting said processed data to the recipient, and

a decoder operated by the recipient for decrypting said encrypted segment.

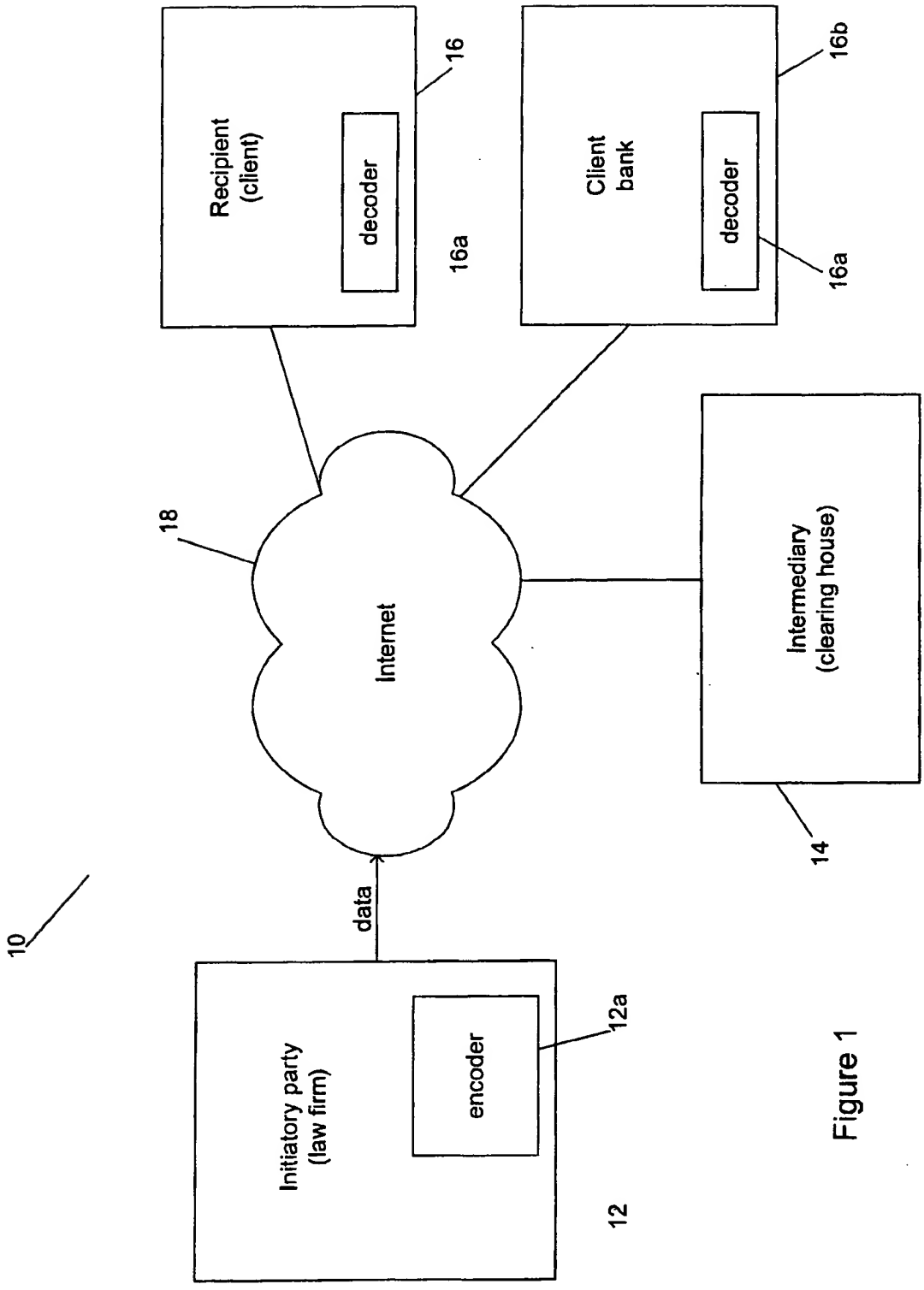

Recipient (client)
decoder
16
16a
Client bank
decoder
16b
16a
18
Internet
Intermediary (clearing house)
14
10
data
Initiatory party (law firm)
encoder
12a
12

Figure 1

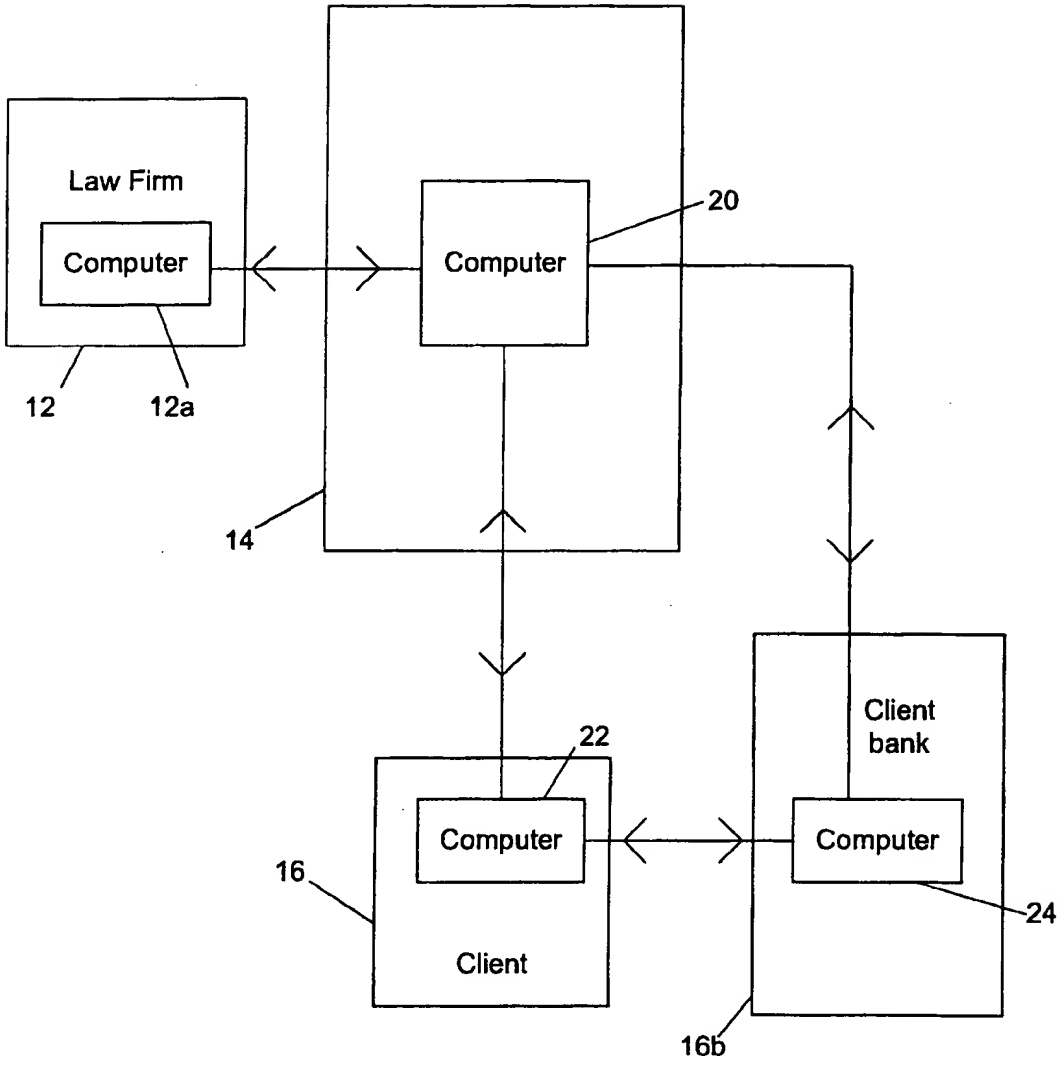

Law Firm
Computer
12
12a
Computer
20
14
Client bank
22
Computer
Computer
16
24
Client
16b

Figure 2